Quick Recovery of Microsoft® Active Directory Using Symantec Backup Exec™ 11d Agent for Active Directory

For use with Microsoft Windows® 2000 Server and Windows Server 2003
Quick Recovery of Microsoft Active Directory Using Symantec Backup Exec 11d Agent for Active Directory

Contents

Executive summary .................................................................4

Traditional Active Directory recovery process ...................................5

Active Directory glossary ..........................................................6

Improving Active Directory backup and recovery .................................6

Backup Exec Agent for Active Directory benefits .................................7

Backup Exec Agent for Active Directory differentiators .........................9

Recovering Active Directory with Backup Exec 11d .................................10

Backup Exec Agent for Active Directory requirements .........................10

Active Directory domain controller requirements ...............................10

Backup Exec 11d media server requirements ....................................11

General requirements and best practices ........................................11

Summary ...............................................................13
Executive summary

Microsoft Active Directory has become the cornerstone of organization and management in Windows-based environments of all sizes that deploy Windows-based systems. It is the standard directory service where applications dependent on Active Directory, such as Microsoft Exchange and SharePoint® Portal Server, are installed. With its increasingly widespread use, the need has intensified for comprehensive data protection and quick recovery of Active Directory.

Human error and hardware or software failures are the leading causes of data and system loss. Active Directory has objects that are sometimes modified or deleted by mistake and attributes that are overwritten by faulty scripts. Also, the Active Directory database can be corrupted as a result of hardware failure. An accidentally deleted user account translates into a loss of user productivity for hours, or even days, while that user is unable to access company resources. Furthermore, Microsoft application dependence on Active Directory exacerbates the risks associated with Active Directory downtime. The loss or corruption of Active Directory data can create a ripple effect across the Windows environment, affecting Microsoft Exchange, SQL Server, and SharePoint.

Most Active Directory recoveries involve lost, deleted, corrupted, or overwritten user accounts, objects, and attributes. If not quickly resolved, these “small disasters” can quickly escalate. When an individual user account, object, or even an individual attribute is lost or corrupted, however, recovery of the entire Active Directory is not practical in terms of administrative time and effort.

Existing recovery solutions for Active Directory typically fall into two categories:

- Standalone utilities requiring backups of Active Directory that are managed separately from existing backups
- Command-line utilities included free with the Windows operating system

Symantec Backup Exec 11d provides an Agent for Microsoft Active Directory that dramatically reduces the time to recover from small disasters, helping to improve employee productivity, reduce the potential for greater issues, and alleviate the aggravation associated with traditional Active Directory protection and recovery.
Traditional Active Directory recovery process

Any administrator who has ever had to restore Active Directory data such as deleted user accounts and lost attributes using standard tools such as Microsoft Ntdsutil understands the time and frustration involved with the current recovery process. Administrators and companies recovering Active Directory data using current Active Directory recovery tools face several limitations:

- Active Directory authoritative restores require the use of command-line system tools such as Ntdsutil.
- A full restore of the system state must be performed, which increases downtime.
- The domain controller must be disconnected from the network for authoritative restores, which prevents users from accessing network resources during recovery.
- The domain controller must be rebooted at least twice, creating additional downtime and risk.
- After full recovery, Active Directory installations that have redundancy through replication must wait for large portions of the directory to replicate inbound and outbound, creating additional downtime.

Traditional recovery for an Active Directory authoritative restore in case of corruption or deletion usually means multiple time-consuming reboots and using complex command-line utilities on a critical Domain Controller. This process is as follows:

1. Reboot in Active Directory recovery mode (F8).
2. Restore system state.
3. Pull network cable.
4. Reboot.
5. Use command-line utility Ntdsutil to elevate objects to recover.
6. Attach to network.
7. Wait for outbound and inbound replication to occur.
Active Directory glossary

Active Directory—Network-based, distributed, hierarchical, replicated object store and service that locates and manages resources.

Active Directory Application Mode (ADAM)—Lightweight version of Active Directory.

Attribute—Property of an Active Directory object (for example, CN = Bob).

Deleted object store—Container that holds objects deleted from Active Directory.

Domain controller—Houses the Active Directory database and responds to security authentication requests (logging in, checking permissions, and so on).

GUID—Global unique identifier.

Object—Resource, service, or person—objects are organized in a hierarchical fashion in Active Directory.

SID—Security identifier (unique).

Tombstone—Indicator used by Active Directory showing that an object is marked for deletion.

Tombstone lifetime—Number of days an object will remain in the deleted object store before deletion.

Improving Active Directory backup and recovery

The Symantec Backup Exec 11d for Windows Servers Agent for Active Directory is licensed as a separate, add-on component on a per-domain-controller basis. It also includes a Remote Agent for Windows Servers license for protecting non–Active Directory data on the domain controller.

The Backup Exec 11d for Windows Servers Agent for Active Directory allows you to recover from inadvertent deletions or changes to Active Directory data in as little as seconds or minutes. Using this new Agent, you can restore Active Directory or Active Directory Application Mode (ADAM) objects and attributes without performing an authoritative or nonauthoritative full restore—and without rebooting.

Simply perform normal System State full backups of your Windows 2000 or 2003 Active Directory domain controllers locally or across the network. The Active Directory Agent’s online,
granular, restore capability then allows you to recover selected objects including users, organizational units, printers, etc, down to the individual attribute level inside of those objects, specific sections of the directory, or the entire Active Directory without taking any Active Directory domain controllers offline.

The Active Directory backup and recovery process is simple by comparison:

1. Select System State components on your Active Directory domain controller(s) for backup.
2. Ensure the checkbox to enable granular restore is selected (enabled by default).
3. Initiate the backup.
5. Select objects or attributes to recover.
6. Initiate the restore.

**Backup Exec Agent for Active Directory benefits**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online recovery</td>
<td>• Recover important Active Directory information while Active Directory is</td>
<td>• Faster, simpler recovery</td>
</tr>
<tr>
<td>(no reboots required)</td>
<td>online</td>
<td>• No rebooting of critical domain controllers to restore lost or damaged</td>
</tr>
<tr>
<td></td>
<td>• No reboots required into Active Directory Services mode for restores</td>
<td>Active Directory objects</td>
</tr>
<tr>
<td></td>
<td>• Supports reanimating “tombstoned” objects in Windows Server 2003 Active</td>
<td>• No impact on network users from loss of domain controller</td>
</tr>
<tr>
<td></td>
<td>Directory environments</td>
<td>• Allows deleted objects to be brought back with their original IDs and correct</td>
</tr>
<tr>
<td></td>
<td>• Maintains SID and GUID information of reanimated “tombstoned” objects in</td>
<td>links to other Active Directory objects, eliminating the need to re-create the IDs</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 Active Directory environments</td>
<td>and thus break those links</td>
</tr>
<tr>
<td>Granular recover</td>
<td>• Restore individual Active Directory objects including deleted user counts,</td>
<td>• Restore only the Active Directory objects you want, when you want</td>
</tr>
<tr>
<td></td>
<td>printers, and organizational units, down to the individual attribute level</td>
<td>• Faster recovery time of individual objects versus entire Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Restore individual objects without restoring the entire Active Directory</td>
<td>• Increased ability to quickly recover the most critical Active Directory objects</td>
</tr>
<tr>
<td></td>
<td>• Recover objects in most Active Directory partitions, including the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration partition</td>
<td></td>
</tr>
<tr>
<td>Full disaster recovery</td>
<td>• Supports complete backups of all system state components, including Active</td>
<td>• Provides full disaster recovery support of system state and Active Directory for fast and easy domain controller recovery</td>
</tr>
<tr>
<td>support</td>
<td>Directory, SYSVOL, COM+ database, Windows registry, and system files</td>
<td></td>
</tr>
</tbody>
</table>
Backup Exec Agent for Active Directory benefits continued

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup and restore performance</td>
<td>• No separate jobs required for database and object-level recovery</td>
<td>• Obtain the benefits of individual Active Directory object-level recovery from high-performance backups of system state</td>
</tr>
<tr>
<td>Ease of management</td>
<td>• Provides an easy-to-use intuitive interface designed for Windows data protection</td>
<td>• Helps reduce training and administrative costs</td>
</tr>
</tbody>
</table>
| Active Directory Application Mode (ADAM) support | • Supports backup and recovery of ADAM objects                              | • Recover ADAM objects as easily as other Active Directory objects using the same Granular Recovery Technology  
• Online ADAM backup and restores                                                                 |                                                                                                                                                                                                                                                                         |
|                                              | • Centralized Active Directory backup and recovery                           | • Perform all restore operations from one central location without going to the domain controller  
• Single console for managing backups for the entire Active Directory environment  
• Integrated Active Directory protection and individual object recovery of your entire environment, including Microsoft Exchange, SharePoint, and SQL Server |                                                                                                                                                                                                                                                                         |
| Single point of administration (centralized management) | • Supports backups to disk or tape¹                                      | • Almost any backup device can be used for protecting Active Directory  
• Active Directory backups can be staged to disk initially for quick recovery and then to tape for offsite disaster recovery protection                                                                                                                                 |
|                                              | • Supports automatic disk-to-disk-to-tape staging¹                          |                                                                                                                                                                                                                                                                                                                                 |
| Media independence                           | • Secure your company’s sensitive Active Directory data with industrial-strength 128-/256-bit AES encryption, included at no additional charge² | • Helps ensure Active Directory backup information is stored securely both onsite and offsite                                                                                                                                                                                                                                          |
| Built-in encryption                          | • Centralized Active Directory backup and recovery                           |                                                                                                                                                                                                                                                                                                                                 |

¹ Granular recovery of individual Active Directory objects from tape backups requires a two-stage restore process. Backup Exec automates this process by staging the data to restore to disk first and then writing the data to the intended restore target location.  
² Encrypted backups are automatically de-encrypted when backed up to disk when Granular Recovery functionality is enabled. Backups can then be encrypted when moved to tape for long-term data protection or disaster recovery purposes.
Backup Exec Agent for Active Directory differentiators

Unlike other solutions, the Backup Exec 11d Agent for Active Directory works with your backups of the Windows system state (where Active Directory is installed) and ADAM. When you back up the Windows system state, Active Directory is included as a component.

To restore individual Active Directory objects and attributes, select them from the View by Resource tab in the Restore Job Properties view. You can also restore individual ADAM objects and attributes by selecting individual ADAM objects and attributes. If multiple ADAM instances are backed up, each instance appears under the ADAM node. To perform a full single-pass backup of Active Directory (see Figure 1):

1. Select System State components on your Active Directory domain controller(s) for backup.
2. Ensure the checkbox to enable granular restore is selected (enabled by default).
3. Initiate the backup.

Figure 1. Single-pass backup of system state
Recovering Active Directory with Backup Exec 11d

Recovery is a simple three-step process for an authoritative restore due to corruption or deletion.

1. Browse Backup Exec 11d created backups of a domain controller (see Figure 2).
2. Select objects or attributes to recover.
3. Initiate the restore.

![Figure 2. Selecting Active Directory objects to recover](image)

Backup Exec Agent for Active Directory requirements

While no additional steps are required to configure Backup Exec for granular recovery of Active Directory objects other than those listed above, you must meet the following requirements before you can restore individual objects and attributes using the Agent for Active Directory.

Active Directory domain controller requirements

Use one of the following Windows operating systems on the computer where Active Directory is installed:

- Windows 2000 Server with Service Pack 4 (Note: Does not support reanimation of objects from the Active Directory Deleted Objects container on a Windows 2000 domain controller. Objects must be re-created by Backup Exec during restore. It is recommended that deleted objects be individually restored by a Backup Exec Remote Agent on a Windows Server 2003 domain controller, if one exists in the same domain.)
Windows Server 2003 with Service Pack 1 or later

Windows Server 2003 R2

**Backup Exec 11d media server requirements**

Use a version of the Windows operating system that supports minifilter drivers on the media server that runs the restore job. The following Windows operating systems support minifilter drivers:

- Windows Server 2003 with Service Pack 1 or later.
- It is also recommended that x64 Windows 2003 Active Directory domain controllers be protected by the x64 version of Backup Exec 11d to perform individual object recovery.

**General requirements and best practices**

- Although it is enabled by default, verify that the option Enable the restore of individual objects from Active Directory backups is selected when you create the backup. Individual attributes and properties can be restored from full Active Directory and ADAM backups only if this option is selected. This checkbox is located on the Microsoft Active Directory node of the Backup Job Properties dialog box.

- If the backup is disk based, the restore will take significantly less time than if the backup is to tape. Restoring from tape requires the creation of a temporary hard disk staging location where the data from tape is first copied. A restore from tape takes longer since the entire backup set must be read to extract the selected attributes and properties. Designate a location through the Tools > Options menu in Backup Exec where Backup Exec can temporarily place the objects and attributes that are being restored when you restore from tape. This location must be a local path on the Backup Exec server and should have enough free disk space to store the entire Active Directory database you are backing up. This temporary data will be automatically deleted once the restore is completed, and the disk space will be reclaimed.

- To restore individual Active Directory or ADAM objects and attributes from tape to a 64-bit computer, move the tape to a media server that is running a 64-bit operating system.
To use a backup-to-disk folder as the destination device for the backup, the backup-to-disk folder must reside on a local NTFS volume to the Backup Exec media server.

You must have created a full backup of the System State of your Windows 2000 or 2003 Active Directory domain controllers with the Backup Exec 11d Agent for Active Directory licensed and installed. Backups made with prior versions of Backup Exec or without the Active Directory agent cannot be used for granular object restore purposes.

You must be running Backup Exec Remote Agent for Windows Servers version 11d on the computer where Active Directory is installed.

“Tombstoned” objects can be reanimated from the Active Directory Deleted Objects container if:

– The objects’ tombstone lifetimes have not passed. This means Active Directory backups have a limited useful lifespan for reanimating tombstoned objects. Restores of objects from backups older than your configured tombstone lifecycle cannot be expected to reanimate the object(s) during restore.

– The objects have not been purged from the Deleted Objects container.

– You are restoring to a Windows Server 2003 Service Pack 1 domain controller.

Note: Tombstone lifespan was changed from 60 to 180 days with Windows 2003 Server Service Pack 1, increasing the window of opportunity to reanimate tombstoned objects from backups. It is recommended that Service Pack 1 be installed on all Windows Server 2003 domain controllers from which backups will be taken. This setting can be modified through the Microsoft command-line utility Ntdsutil.
Quick Recovery of Microsoft Active Directory Using Symantec Backup Exec 11d Agent for Active Directory

**Summary**

IT organizations continually strive to implement new efficiencies in protecting and recovering key data in their environment, particularly where sensitive data is concerned. Active Directory has become a key component of organizations with Windows-based systems and the foundation on which other Microsoft applications depend (for example, Microsoft Exchange and SharePoint). Current recovery solutions for Microsoft Active Directory do not provide the capability to handle the most common Active Directory recovery situations, specifically, the recovery of individual objects. Symantec Backup Exec 11d for Windows Servers Agent for Active Directory offers an innovative, new technology to help IT administrators quickly and easily recover the Active Directory data they want, when they want. Best of all, it enables the recovery of key Active Directory user, attribute, and component data in as little as seconds or minutes—without the need for system reboots.
About Symantec
Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.